REMARKS

In view of the above amendments and following remarks, further reconsideration of the present application is respectfully requested.

Claims 1-31 have been cancelled and Claims 32-38 have been newly added. It is submitted no new matter has been added.

A personal interview was conducted with Examiner Aravind K. Moorthy and Primary Examiner Syed Zia on November 16, 2006 at the United States Patent and Trademark Office. During the personal interview, the Applicants' representative set forth arguments traversing the Examiners 35 U.S.C. §112, first paragraph rejection and 35 U.S.C. §103 prior art rejections. As reflected on the Interview Summary form PTO-413, the Examiner has agreed to withdraw the 35 U.S.C. §112, first paragraph rejection. The Examiner also stated that he would reconsider the prior art rejections upon receiving this formal response. Included next is a "Substance of the Interview" which includes arguments presented during the personal interview regarding the shortcomings of the prior art.

The Examiner has rejected Claims 1-12 and 17-31 under 35 U.S.C. §112, first paragraph, for the reasons contained in Paragraph 6 on Page 2 of the Office Action. Particularly, the Examiner has asserted that the following limitation lacks support in the specification: "*the scrambled access information being used by the access device and the storage medium for calculating the first and second response values.*"

The Applicants strongly disagree with the Examiner and traverse the Examiner's 35 U.S.C. §112 rejection. The Applicants submit that the aforementioned limitation is clearly supported by at least the following portions of the application:

- The scrambled access information R1 is used by the access device for calculating a response value V2' = F1(R1, UK) (see [0053], Fig. 2, S103 of Fig. 4).

- The scrambled access information R1 is used by the storage device for calculating a response value V2 = F1 (R1, UK) (see [0087], Fig. 2, S106 of Fig. 4).

Accordingly, as per the Examiner's agreement during the personal interview, the 35 U.S.C. §112 rejection is improper and should not be maintained.

Next, the Examiner has rejected each of independent Claims 1, 11, 12, 17, 19, and 21-23 under 35 U.S.C. §103(a) as being unpatentable over *Kocher et al.* (U.S. Patent NO. 6,289,455) in view of *Hellman* (U.S. Patent No. 5,872,917) for the reasons contained in Paragraph 7 of the Office Action.

The Applicants traverse the Examiner's aforementioned prior art rejection. Nonetheless, in an effort to expedite allowance of this application, the Applicants have cancelled claims 1-31 in favor of newly added Claims 32-38. It is noted that each of newly added independent Claims 35, 35 and 38 have been drafted to more clearly distinguish over the prior art references.

Accordingly, the Applicants strongly submit that each of newly added independent Claims 33, 35 and 38 clearly and patentably distinguishes over the prior art references for at least the following reasons.

Initially, the Applicants traverse the Examiner's obviousness rejection under 35 U.S.C. §103(a) for failure by the Examiner to establish *prima facie* obviousness of the claimed invention. Particularly, the Examiner has failed to meet all three requirements for establishing a prima facie case of obviousness. To establish prima facie obviousness of a claimed invention, one of the three requirement is that all the claim limitations must be taught or suggested by the

prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) [see MPEP 2143.03]. The Examiner states the following on page 4 of the Office Action:

> "*Kocher et al* does not teach that the storage medium is authenticated by a challenge-response authentication protocol (Column 3, Lines 48-551. *Kocher et al.* does not teach that first and second response values are compared.
>
> *Hellman* teaches the challenge-response authentication protocol and its benefits (Column 6 Line 57 to column 8 line 5). *Hellman* teaches that a first and second response is compared (Column 6, Line 57 to Column 8, Line 5).
>
> The scrambled access information would have been used to calculate first and second response values. The first and second response values would have been compared to authenticate the challenge-response protocol."

However, each of the previously pending independent claims recited "the scrambled access information being used by the access device and the storage medium for calculating the first and second response values." As evidenced by the Examiner's last paragraph quoted above, the Examiner has clearly failed to address the claim limitations in which both the access device calculates a response value using the scrambled access information and the storage medium calculates a response value using the scrambled access information. Moreover, the mere fact that the Examiner alleged a lack of support in the specification for the above cited claim language via 35 U.S.C. §112, first paragraph, is irrelevant since, when evaluating claims for obviousness under 35 U.S.C. §103, all the limitations of the claims must be considered and given weight, including limitations which do not find support in the specification as originally filed (i.e., new matter). *Ex part Grasselli*, 231 USPQ 393 (Bd. App. 1983) *affd mem.* 738 F.2d 453 (Fed. Cir. 1984) [see MPEP 2143.03]. It is further noted that the Examiner's 35 U.S.C. §112, first paragraph, rejection was improper and agreed to be withdrawn by the Examiner during the personal interview. Accordingly, it is submitted that the Examiner has failed to establish that the

prior art teaches or suggests all the claim limitations of the previously pending independent claims and, thus, has failed to establish a prima facie case of obviousness. Thus, the 35 U.S.C. §103(a) rejection is improper and should not be maintained.

Next, notwithstanding the fact the Examiner has made an improper obviousness rejection under 35 U.S.C. §103(a), the Applicants submit the prior art references relied upon by the Examiner, either taken alone or in combination, fail to disclose or suggest each and every feature claimed in newly added independent Claims 32, 35 and 38.

According to each of newly added independent claims 32, 35 and 38, the access device transmits, to the storage medium, scrambled access information generated by scrambling access information designating an area in the storage medium used for storing digital information, and authenticating, in the access apparatus, whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information; authenticating, in the storage medium, whether the access apparatus is authorized according to a challenge-response authentication protocol without using the scrambled access information; and reading/writing the digital information from/into the area designated by the access information after the storage medium and the access apparatus have authenticated each other as authorized devices.

For example, in the illustrative embodiment shown in Figures 2 and 4 of the present application, the access device 10 transmits to the storage medium 20 scrambled access information R1 generated by scrambling access information designating an area in the storage medium used for storing digital data, and the access device 10 authenticates whether the storage medium 20 is authorized according to a challenge-response protocol using the scrambled access information R1 [see steps S102-S108 in Figure 4], and the storage medium 20 authenticates

whether the access apparatus is authorized according to a challenge-response protocol without using the scrambled access information [see steps S109-5115 in Figure 4].

By providing the aforementioned features, very secure and effective mutual authentication is performed and the reading/writing of digital information from/into the storage medium can be performed in a quick manner after the storage medium and access device have authenticated each other as authorized devices since the access information designating the area in the storage medium used for storing the digital information can be promptly extracted from the scrambled access information used during authentication of the storage medium.

The Applicants strongly submit that the aforementioned features, which are contained within each of newly added independent Claims 32, 35 and 38, as well as the advantages resultant therefrom, are not disclosed or suggested by the *Kocher et al.* or *Hellman* references, taken either alone or in combination, for at least the following reasons.

Regarding the *Kocher et al.* reference, it is noted that the Examiner relies on Column 19 (lines 36-43) of the *Kocher et al.* reference for allegedly disclosing "a first authentication phase in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area" (see Paragraph 7 on Page 3 of Office Action]. Moreover, the Examiner indicates on Page 4 of the Office Action that, "*Kocher et al* does not teach that the storage medium is authenticated by a challenge-response authentication protocol. "

According to the disclosure of column 19 (lines 36-43) of *Kocher et al.*, the Interface control processor 235 stores an encrypted key in CryptoFirewall's 260 externally accessible register, the encrypted key typically being obtained from a KDM distributed by a content provider with the contents to be decoded. Particularly, as shown in item 205 of Figure 2, the

KDM is transmitted with corresponding content from a content provider 200 to a playback device 210. (See Figure 2, Column 8, Lines 17-21 and Column 19, Lines 36-43). To decode content, playback device 210 transmits the KDM in a control message 220 to a cryptographic rights unit 225 containing a CryptoFirewall 260 which derives and returns one or more content decryption keys 267 to the playback device 210 for decrypting content 215 (see Figure 2 and Column 9, Lines 41-48). The CryptoFirewall 260 regulates data written to, or read from, a protected memory (Column 10, Lines 5-6). The CryptoFirewall 260 implements a set of operations including adding new rights by pre-payment (Figure 3), adding new rights for post-payment (Figure 4), accessing content (Figure 5), auditing/clearing post-paid purchase audit records (Figure 6), and renewing rights (Figure 7) (see Figures 3-7 and Column 10, Lines 25-35)]. During such operations, although Kocher et al. discloses the transmission of address information from the interface control processor 235 to the CryptoFirewall 260 for purposes of verification/validation of the addresses (see for example, see 330 in Fig. 3, 430 in Fig. 4, 520 in Figure 5, 620 in Figure 6, and 720 in Figure 7), it is submitted that *Kocher et al.* fails to disclose or suggest the transmission of scrambled access information from an access device to the storage medium, the scrambled access information generated by scrambling access information designating an area in the storage medium used for storing digital information, and authenticating, in the access apparatus, whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information and authenticating, in the storage medium, whether the access apparatus is authorized according to a challenge-response authentication protocol without using the scrambled access information, as recited in newly added independent Claims 32, 35 and 38. Moreover, unlike newly added independent claims 32, 35 and 38 which recite the reading/writing of digital information

from/into the area designated by the access information after the storage medium and the access apparatus have authenticated each other as authorized devices, the *Kocher et al.* reference, as described above, discloses performing the reading/writing of data at the same time as authentication of the *Kocher et al.* system is performed.

Next, regarding the *Hellman* reference, it is noted that the Examiner has merely stated, on Page 4 of the Office Action, that "*Hellman teaches the challenge-response authentication protocol and its benefits (Column 3, Lines 48-55).*" While it is correct that *Hellman* teaches a challenge-response authentication protocol, the *Hellman* reference does not teach the particular features which are being claimed in newly added independent Claims 32, 35 and 38. Particularly, *Hellman* fails to disclose or suggest an access device transmitting to a storage medium scrambled access information generating by scrambling access information designating an area in the storage medium used for storing digital information, as recited in each of newly added independent Claims 32, 35 and 38. Instead, as clearly shown in Figure 1, *Hellman* merely discloses a user computer transmitting a user ID 16 to a host computer (see Figure 1 and Column 6, Lines 35-39). Next, since the *Hellman* reference does not disclose the transmission of such scrambled access information, it is clear that *Hellman* does not disclose authenticating, in the access apparatus, whether a storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information, as recited in independent Claims 32, 35 and 38. Instead, *Hellman* merely discloses the comparison of a user value (UV) and a host response (HR) each which are generated using a password, a challenge 18 and an extra value of a known format (PAD) (see Figure 1 and Column 7, Line 62 through Column 8, Line 2). Finally, the *Hellman* reference fails to disclose or suggest reading/writing digital information from/into the area designated by the access information after the storage medium and the access

apparatus have authenticated each other as authorized devices, as recited in newly added independent claims 32, 35 and 38. Instead, *Hellman* merely discloses that if the (UV) and (HR) do not match, then the authentication sequence aborts, and if the (UV) and (HR) match, then the identity of the host is verified and the user may begin or continue a work session (see Column 7, Line 67 through Column 8, Line 5).

Lastly, as a motivation for combining the *Kocher et al.* and *Hellman* references, the Examiner has stated, on page 4 of the Office Action, that "*It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kocher et al by the teaching of Hellman because the security of authentication, based on the addition of PAD, is improved even when relatively short passwords are used.*" The Applicants note that such a proposed combination including the PAD actually teaches away from the present invention. Particularly, the extra value PAD generated at the user computer is NOT transmitted to the host computer (see Column 7, Lines 4-7). On the contrary, according to the invention claimed in each of newly added independent Claims 32, 35 and 38, the scrambled access information is in fact transmitted from the access device to the storage medium in order to allow the access device to quickly read/write data from/into the address shown by the access information after the storage medium and the access device have authenticated each other.

Accordingly, the Applicants strongly submit that the *Kocher et al.* and *Hellman* references, taken either alone or in combination, fail to disclose or suggest each and every feature recited in newly added independent Claims 32, 35 and 38.

Moreover, it is strongly submitted that none of the numerous other references previously cited and/or relied upon by the Examiner teach of suggest the aforementioned shortcomings of

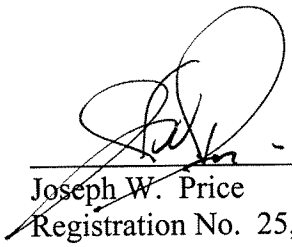
the *Kocher et al.* and *Hellmann* references as recited in newly added independent Claims 32, 35 and 38.

Since only allowable subject matter is now pending in the application, an early notification of allowance is respectfully requested.

If the Examiner believes a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed phone number.

Very truly yours,

SNELL & WILMER L.L.P.



Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799